

Opening Statement for Subcommittee Ranking Member Brian Higgins (D-NY)

Subcommittees on Counterterrorism & Intelligence and Cybersecurity, Infrastructure Protection & Security Technologies

“Assessing Persistent and Emerging Cyber Threats to the U.S. Homeland”

May 21, 2014

I would like to thank the Chairman for holding today’s hearing. I look forward to hearing the testimony of our witnesses as the Committee continues to expand our interests and understanding of the current and evolving cyber threats. I have gone on record before to state that cyber threats know no limits and have no boundaries. As a Member representing the Buffalo and Niagara region, I dedicate a significant amount of my time and interests to issues related to border security and the facilitation of commerce.

However, I understand the threats to our country and our way of life are not limited to the reach of planes, trains, and automobiles and also that these threats cannot be contained by Congressional districts. As technology continues to mature and our online world continues to grow, the threats and the means to carry out those threats grow as well. For the second consecutive year, the Director of National Intelligence, James Clapper has designated cybersecurity as the top global threat. Also, the number two global threat for the U.S. on this same list is related to concerns of espionage.

As a reflection of the growing espionage cyber threats, on Monday, for the first time in U.S. history, the Department of Justice issued indictments related to cyber security against foreign state actors. Pursuant to that indictment, five members of the Chinese military were charged with a total of 155 counts of crimes related to computer hacking, economic espionage and other offenses related to cybersecurity. I believe this indictment sends a strong message for state-actors that the U.S. will not be intimidated by cyber hackers and we will remain vigilant against attempts against cyber espionage. While I understand that the unprecedented nature of this indictment has and will continue to interest members of this committee and Congress as a whole, I will refrain from interfering with the ongoing judicial process.

However, I would request that as information can be shared with us, our witnesses will return to brief members of this committee in the appropriate setting. America’s economic prosperity depends on cyber security, and that is why we need effective oversight and robust cyber legislation that includes strategic initiatives, including public-private partnerships that protect our nation from hackers, nefarious state actors, and foreign intelligence services from countries such as China.

While I understand that it would be inappropriate for our witnesses to go into detail about specific cyber threats in this open setting; when possible, I believe an open discussion of the threats that we do know about, the technologies being used, and massive vulnerabilities can be helpful to the American public. It is clear to everyone that our dependence on technology is growing exponentially by the day.

Therefore our nation depends on us, both Congress and Federal agencies and departments to have a robust, comprehensive set of cybersecurity policies and procedures in place. Therefore, we must not only examine the threat, but also protect critical infrastructure and safeguard our personal and financial information, while promoting research and development to ensure that we have the proper protocols in place.